(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平6－509927

第７部門第３区分　(43)公表日　平成６年(1994)11月２日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		
Ｈ０４Ｌ　29/06					
Ｇ０６Ｆ　11/30		３２０　Ｇ	9290－5B		
13/00		３５３　Ｕ	7368－5B		
			9371－5K	Ｈ０４Ｌ　13/00	３０５　Ｚ
			9371－5K		３１１

審査請求　未請求　予備審査請求　未請求(全 13 頁)　最終頁に続く

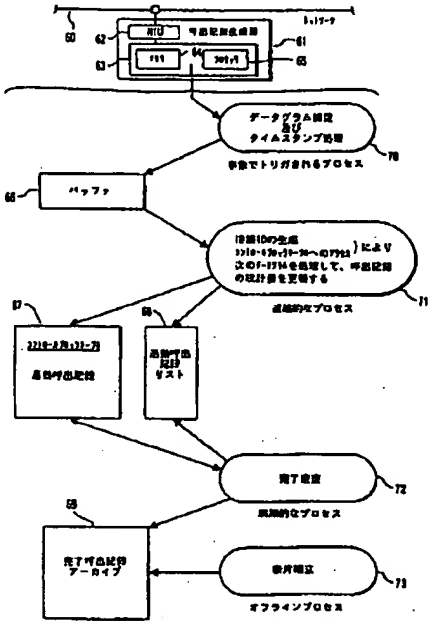
(21)出願番号　特願平6－501208
(86)(22)出願日　平成４年(1992)６月17日
(85)翻訳文提出日　平成６年(1994)２月17日
(86)国際出願番号　ＰＣＴ／ＧＢ９２／０１０９０
(87)国際公開番号　ＷＯ９３／２６１１１
(87)国際公開日　平成５年(1993)12月23日
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＳＥ)，ＪＰ，ＵＳ

(71)出願人　ヒューレット・パッカード・カンパニー
アメリカ合衆国カリフォルニア州94304パロ・アルト，ハノーバー・ストリート・3000
(72)発明者　ガローヴェイ，ジェイムズ，ロバートソン
ドイツ国7038ホルツガルリンゲン，ヤーン・シュトラーセ・16
(74)代理人　弁理士　古谷　馨　(外２名)

(54)【発明の名称】　ネットワーク監視方法及び装置

(57)【要約】　（修正有）

プロトコルデータユニットを送るためにエンティティの各対の間でネットワーク（６０）に亘って一時的に確立される通信接続を監視するためのネットワーク監視方法及び装置（６１）が開示されている。その接続は、例えば、TCP／IPプロトコルセットに従って実施される。本方法は、ネットワークを監視して、プロトコルデータユニットと、その各プロトコルデータユニットが関連する接続とを識別し、現在活動状態であるとみなされる個々の接続を各々が表す呼出記録からなる活動グループ（６７）を維持する、というステップを含む。この呼出記録からなる活動グループ（６７）の維持は、プロトコルデータユニットが活動グループ（６７）中で表されることのない接続に関連するものとして識別される毎に活動グループ（６７）に新たな呼出記録を加え、更に別のプロトコルデータユニットが活動グループ（６７）中の既存の呼出記録により表される接続に関連するものであると識別されることに応じてその既存の呼出記録を更新し、既存の呼出記録に対応する接続に関連する更なるプロトコルデータユニットが継続的に存在しないことに関



してその接続が完了しているものと判定された際に、その接続を活動グループから呼出完了グループ（６９）へ除去することにより行われる。

請求の範囲

１．プロトコルデータユニットを送るためにエンティティの各対の間でネットワークに亘り一時的に確立される通信接続を監視する方法であって、前記ネットワークを介して送られる各プロトコルデータユニットは、送信側エンティティにより、その送信側エンティティが関連する接続を識別する関連接続情報と共に提供され、前記方法が、前記ネットワークを監視して前記プロトコルデータユニットとそのような各プロトコルデータユニットが関連する接続とを識別し、現在活動状態であるとみなされる個々の前記接続を各々が表す呼出記録からなる活動グループを維持するというステップを含み、この維持ステップが、

プロトコルデータユニットが前記活動グループ中で表されることのない接続に関連するものと識別される毎に、新たな呼出記録を前記活動グループに加え、

別のプロトコルデータユニットが前記記録により表される接続に関連するものと識別されたことに応じて、前記活動グループ中の既存の呼出記録を更新し、

前記接続に関連する更なるプロトコルデータユニットが継続的に存在しないことに関してその接続が完了しているものと判定された際に、前記活動グループから既存の呼出記録を除去するというステップを含む、前記方法。

２．前記活動グループ中の各呼出記録に、記録が生成された際及び記録が更新された際に設定される個々の活動標識が設けられており、前記活動グループの呼出記録を間隔をおいてチェックし、前記活動標識がリセット状態にある記録をその都度除去し、その他の呼出記録の活動標識をリセットすることにより、前記活動グループからの呼出記録の除去を行うことを特徴とする、請求項１記載の方法。

３．前記活動グループから除去される前記呼出記録を呼出完了記録グループとして維持する、請求項１または請求項２記載の方法。

４．前記プロトコルデータユニットの少なくとも幾つかが、その関連する接続の進捗に関連する関連制御コードを有し、前記ネットワークの監視ステップが、前記プロトコルデータユニットに関連する前記制御コードを識別するというステップを含み、前記維持ステップが、前記活動グループの各呼出記録毎に、その記録により表される接続に関連する前記制御コードを前記記録の一部として格納するというステップを含み、更にこの方法が、同じ一対のエンティティ間の接続に関する記録について呼出完了グループの呼出記録を走査し、そのような記録中に格納されている前記制御コードから、前記記録が同じ接続の部分的な記録を構成するものであるか否かを判定し、前記記録が同じ接続の部分的な記録を構成するものである場合に前記記録を組み合わせるというステップを含む、請求項３記載の方法。

５．前記活動グループの各呼出記録が、記録の生成時に設定されて、対応する接続の開始時間を示す、呼出開始情報項目と、前記記録に関連するものと引き続いて識別された各プロトコルデータユニット毎に更新されて、対応する接続の潜在的終了時間を示す、呼出終了情報項目とを含む、請求項１記載の方法。

６．前記ネットワーク監視ステップが、そのステップで識別された各プロトコルデータユニットに個々のタイムスタンプを関連させるというステップを含み、前記各呼出記録の呼出開始情報項目が、呼出記録を生成させるプロトコルデータユニットのタイムスタンプに設定され、同じ記録の呼出終了情報項目が、その記録により表される接続に関連するものであると識別された各々の連続的なプロトコルデータユニットのタイムスタンプに設定される、請求項５記載の方法。

７．前記プロトコルデータユニットの少なくとも幾つかが、その関連する接続の確立に関する関連制御コードを有し、前記ネットワーク監視ステップが、前記プロトコルデータユニットに関連する前記制御コードを識別するというステップを含み、前記維持ステップが、前記活動グループに加えられる各呼出記録毎に、その記録により表される接続に関連する前記制御コードから、その接続に関連する前記一対のエンティティのうちの何れのエンティティがその接続を開始させたかを決定し、その開始エンティティの同一性を前記呼出記録中に格納するというステップを更に含む、請求項１記載の方法。

８．前記ネットワーク監視ステップが、前記の識別された各プロトコルデータユニット毎に、そのプロトコルデータユニットに関する定量情報を両方とも決定するというステップを更に含み、その方向に、そのプロトコルデータユニットが関係する前記接続に関連する

前記一対のエンティティの間で前記プロトコルデータユニットが送られており、前記維持ステップが、前記一対のエンティティの間の前記方向の各々に関するプロトコルデータユニットについてのそれぞれの組合された前記定量情報を前記各呼出記録が含むようにしたものである、請求項1記載の方法。

9．各プロトコルデータユニットの前記関連接続情報が、そのプロトコルデータユニットが関係する接続に関連する前記一対のエンティティの各々のネットワークアドレスを含み、前記ネットワーク監視ステップが、前記関連接続情報に含まれるネットワークアドレスから接続識別子を形成することにより前記各プロトコルデータユニットが関連する前記接続を識別するというステップを含み、前記の接続識別子の形成が、前記エンティティ間でのプロトコルデータユニットの通過方向に左右されない形態を前記接続識別子が有するような態様で行われ、その接続識別子を前記維持ステップで使用して、対応する前記呼出記録を識別する、請求項1記載の方法。

10．前記維持ステップが、前記活動グループの前記呼出記録をハッシュテーブルに格納し、特定のプロトコルデータユニットに関連する前記接続識別子から形成されたハッシュキーを用いることにより、前記の特定のプロトコルデータユニットに関する呼出記録に前記ハッシュテーブル中でアクセスするというステップを含む、請求項9記載の方法。

11．前記接続がTCP/IPプロトコルセットに従って実施されている、請求項1ないし請求項10の何れかに記載の方法。

12．プロトコルデータユニットを送るためにエンティティの各対の間でネットワークに亘って一時的に確立される通信接続を監視する装置であって、前記ネットワークを介して送られる各プロトコルデータユニットは、送信側エンティティにより、その送信側エンティティが関連する接続を識別する関連接続情報と共に提供され、前記装置が、前記ネットワークを監視して前記プロトコルデータユニットとその各プロトコルデータユニットが関連する接続とを識別する監視手段と、この監視手段に接続され、現在活動状態であるとみなされる個々の接続を各々が表す呼出記録からなる活動グループを維持するよう動作する呼出記録手段とを含み、この呼出記録手段が、

前記呼出記録からなる前記活動グループを格納する格納手段と、

前記の各プロトコルデータユニットが関連する前記接続が、前記監視手段により識別された際に、その接続が前記活動グループ中の前記呼出記録により表されるか否かを判定し、前記接続が前記呼出記録により表されないものであると判定された場合に、前記活動グループに新たな呼出記録を加える、記録生成手段と、

更に別のプロトコルデータユニットが、前記活動グループ中の既存の呼出記録により表される接続に関連するものであると前記監視手段により識別されたことに応じて、その呼出記録を更新する、記録更新手段と、

前記接続に関連する更なるプロトコルデータユニットが継続的に存在しないことに関してその接続が完了しているものと判定された際に、前記活動グループから既存の呼出記録を除去する、記録除去手段とを含んでいることを特徴とする装置。

明細書

ネットワーク監視方法及び装置

技術分野

本発明は、ネットワークにわたって配設される通信接続を監視する方法及び装置に関し、特に（これに限定されるものではないが）、TCP／IPプロトコルに従って実施される接続に関する呼出記録の生成に関するものである。

背景技術

データ通信ネットワークを介して互いに通信を行うエンティティは、一般に所定のプロトコルに従ってデータ・パケットを交換することによりその通信を行う。使用される特定のプロトコルに応じて、エンティティ間で提供される通信サービスは、一般に、無接続型、又は接続指向型の何れかとなる。無接続型サービスとは、各パケットが他のあらゆるパケットから分離されて処理されるサービスであり、このサービスは、パケットが、一緒になって完全なメッセージを形成する多数のパケットのうちの一つであるか否かを認識することはない。これに対し、接続指向型サービスは、エンティティ間を通過するパケットのための高信頼性のストリーム伝送サービスを提供するために、通信を所望するエンティティ間に仮想回線を確立する。この仮想回線は、エンティティが相互の通信を完了した際に閉じられ、この仮想回線を介してエンティティ間で確立される上記の

ような通信経路は、一般に接続と呼ばれ、また、接続の単個から遮断までに実行される通信トランザクションは「呼出」と呼ばれることが多い。

トラフィックの監視目的及び故障分析の目的の双方のためにネットワーク監視装置を設けることは公知である。このような監視装置は、その殆どが、個々のパケットの分析、又は監視されるパケット全体の総合効果に関するものである（例えば、トラフィック推定、ネットワーク計画に関するもの）。米国特許第5,101,402号明細書には、接続を介して伝達されるセションについての統計量の収集を提供するやや精巧な方法が開示されている。しかし、この米国特許第5,101,402号明細書に開示の方法は、各セションの終了時を確認するために、セションプロトコル対話を追跡しなければならない、という欠点を有する。その結果、セションを終了させる関連プロトコル指令の通過が何らかの理由（ノイズやパケットの再経路指定等）で欠落した場合には、エラー状態が生じることになる。

本発明の目的は、パケットの損失に対して柔軟性を有する、ネットワークに亘る呼出を監視する方法及び装置を提供することにある。

発明の開示

本発明の一態様によれば、プロトコルデータユニットを双方の間に送るためにエンティティの各対の間でネットワークに亘って一時的に確立される通信接続を監視する方法が提供される。ここで、ネットワークを介して通過する各プロトコルデータユニットは、送信側エンティティにより、その送信側エンティティが関連する接続を識別する関連接続情報と共に提供される。本方法は、前記プロトコルデータユニットとその各ユニットが関連する接続とを識別するためにネットワークを監視し、現在活動状態であるとみなされる個々の前記接続を各々が表す呼出記録からなる活動グループを維持する、というステップを含み、前記維持ステップは、

前記プロトコルデータユニットが、前記活動グループ中で表されることのない接続に関連するものであると識別される毎に、新たな呼出記録を前記活動グループに加え、

更に別のプロトコルデータユニットが、前記活動グループ中の既存の呼出記録により表される接続に関連するものであると識別されたことに応じて、その既存の呼出記録を更新し、

前記接続に関連する更なるプロトコルデータユニットが継続して存在しないことに関連して前記接続が完了しているものと判定された際に、前記活動グループから前記の既存の呼出記録を除去する、というステップを含む。

一般に、活動グループから除去された呼出記録は、呼出完了記録グループとして保持され、これにより、実行された呼出の履歴記録が提供される。更に、各呼出記録は、通常は、呼出記録が関連する接続に含まれる一対のエンティティ間のデータフローの各方向に関するプロトコルデータユニットについての総合定量情報（例えば、伝送されたデータバイト数）を記録する。

各プロトコルデータユニットの前述の関連接続情報は、例えば、プロトコルデータユニットが関係する接続に関連する一対のエンティティの各々のネットワークアドレスを備えることができる。この場合、ネットワークを監視するステップは、好適には、関連接続情報に含まれるネットワークアドレスから接続識別子を形成することにより、各プロトコルデータユニットが関連する接続を識別する、というステップを含む。前記の接続識別子を形成は、エンティティ間でのプロトコルデータユニットの通過方向に左右されない形態を前記接続識別子が有するような態様で行われ、その接続識別子が前記維持ステップで使用されて、対応する呼出記録が識別される。

活動グループからの呼出記録の除去を容易化するために、その活動グループ中の各呼出記録には、好適には、記録が生成された際、及び記録が更新された際に設定される個々の活動標識が与えられる。次いで、活動グループの呼出記録を周期をおいてチェックし、活動標識がリセット状態にある記録をその都度除去し、残りの呼出記録の活動標識をリセットすることにより、活動グループからの呼出記録の除去が行われる。

プロトコルデータユニットの少なくとも幾つかが、その関連する接続の進捗に関連する関連制御コードを有している場合には、ネットワークの監視ステップは、好適には、これらの制御コードを識別し、それらを関連する呼出記録の一部として格納する、というステップを含む。これは、次いで同じ一対のエンティティ間の接続に関する記録について呼出完了グループの呼出記録を走査し、そのような記録に格納されている制御コードから、その記録が同じ接続の部分的な記録として互いに適合するものであるか否かを判定することにより、別個の呼出として誤って識別された呼出断片を引き続いて互いに継ぎ合わせることを可能にする。

好適には、各呼出記録は、対応する接続の開始時間を示すためにその記録の生成時に設定される呼出開始情報項目と、対応する接続の潜在的終了時間を示すために引き続いて前記記録に関連するものとして識別された各プロトコルデータユニット毎に更新される呼出終了情報項目とを含んでいる。この目的のため、ネットワークの監視ステップは、好適には、そのステップで識別された前記の各プロトコルデータユニットに個々のタイムスタンプを関連させることを含む。次いで、各呼出記録の呼出開始情報項目が、呼出記録を生成させるプロトコルデータユニットのタイムスタンプに設定され、同じ記録の呼出終了情報項目が、関連する接続に関するものであると識別された各々の連続的なプロトコルデータユニットのタイムスタンプに設定される。

前記プロトコルデータユニットの少なくとも幾つかが、それらに関する接続の確立に関連する関連制御コードを有している場合、各呼出記録は、対応する接続を開始させるエンティティの同一性を含むことができ、プロトコルデータユニットと関連する制御コードにより、１つの接続に関する２つの通信エンティティのうちの何れがその接続を開始させたかを示す働きをする活動グループに、新たな呼出記録が加えられる。

本発明の別の態様によれば、プロトコルデータユニットを双方の間に送るための個々の一対のエンティティ間のネットワークに亘っ

て一時的に確立される通信接続を監視する装置が提供される。ここで、ネットワークを介して通過する各プロトコルデータユニットは、送信側エンティティにより、その送信側エンティティが関連する接続を識別する関連接続情報と共に提供される。本装置は、前記プロトコルデータユニットとその各ユニットが関連する接続とを識別するためにネットワークを監視する監視手段と、この監視手段に接続され、現在活動状態であるとみなされる個々の前記接続を各々が表す呼出記録からなる活動グループを維持するよう動作する呼出記録手段とを含み、この呼出記録手段が、

呼出記録からなる前記活動グループを格納する格納手段と、

前記プロトコルデータユニットの各々が関連する前記接続が前記監視手段により識別された際に、その接続が前記活動グループ中の前記呼出記録により表されるか否かを判定し、前記接続が前記呼出記録により表されないものであると判定された場合に、前記活動グループに新たな呼出記録を加える、記録生成手段と、

更に別のプロトコルデータユニットが、前記活動グループ中の既存の呼出記録により表される接続に関連するものであると前記監視手段により識別されたことに応じて、その既存の呼出記録を更新する、記録更新手段と、

前記接続に関連する最後のプロトコルデータユニットの識別時に関して、前記接続が非活動状態にあると判定された場合に、前記活動グループから既存の前記呼出記録を除去する、記録除去手段とから構成されている。

本発明の方法及び装置は、TCP／IPプロトコルセットを用いて通信が行われる場合の呼出記録生成に特に適するものである。

図面の簡単な説明

本発明を実施した呼出記録生成装置及び本発明によるネットワーク監視方法を、非制限的な例により、添付図面を参照して特に説明することとする。

図１は、２つの通信エンドシステムのプロトコルスタックを示す図である。

図２は、TCP／IPプロトコルセットに従って通信エンティティ間で伝送されるデータのカプセル化を示す図である。

図３は、TCP／IP接続のオープン及びクローズ中におけるエンドシステム間での制御メッセージの交換を示す図である。

図４は、ネットワーク監視方法で用いられる主な処理及びデータ構造を示す図である。

図５は、ネットワーク監視方法の間に構築される呼出記録の内容を示す図である。

図６は、図４に示す「次のデータグラムの処理」プロセスを示すフローチャートである。

図７は、図４に示す「完了走査」プロセスを示すフローチャートである。

発明を実施するための最良形態

添付図面中、図１は、ネットワーク12を介して互いに通信を行う際に２つのエンドシステムにより操作される概念的なプロトコルスタック1,2を示している。各プロトコルスタック1,2は、通信プロセスにおいて特定のタスクを各々が実行する多数の異なる層から構成されている。例示のため各プロトコルスタック1,2中の層Nを考察すると、この層Nは、(層N+1)の上位の層に対してサービスを行い、その際に、(層N-1)の下位の層により提供されるサービスを利用する。

各層N中で、プロトコルエンティティ3,4は、その各層に割り当てられた通信タスクの実行を制御する。この制御は、通信エンドシステムの対応するプロトコルエンティティとの協調をとって行われる。概念的には、通信エンドシステムの同じプロトコル層中のプロトコルエンティティ3,4は、対等(peer)プロトコル（層Nの場合、これは図１に示す層Nのプロトコルである）に従って、互いに通信及び協調を行う。対等プロトコルは、対等プロトコルエンティティ3,4間で送られるメッセージの形式及びシーケンスをプロトコルデータユニット5,6という形で規定する。各プロトコルデータユニット(PDU)5,6は、プロトコル制御情報PCIと、１つ以上のサービスデータユニットSDUとを含み、後者は、層Nのプロトコルエンティティが上位層N+1のために操作するデータである。

概念的には、対等プロトコルエンティティ3,4は、その相互間で直接的にプロトコルデータユニットを送ることによって互いに通信を行うが、実際には、プロトコルデータユニットは、ネットワーク12を介して関連する層Nに関して、１つのプロトコルスタックを下位へ送り、他のプロトコルスタックを上位へ送らなければならないことはいうまでもない。層Nのプロトコルエンティティにより層N-1へと下位へ送られたプロトコルデータユニットは、その層N-1によりサービスデータユニットSDUとして扱われて適当に操作される。

このような通信プロトコルスタックの概念的層状化は、当業界で公知である。例えば、国際標準化機構（国際標準ISO7498）により規定された7層OSI（開放型システム相互接続）モデルを参照されたい。低レベルは専用ハードウェアを使用して十分達成可能であるが、実際にはプロトコルスタックは主にソフトウェアで実施される、ということが理解されよう。

各対等プロトコルの形式は、無接続型又は接続指向型の何れかである。対等プロトコルNが無接続型の場合、関連するプロトコルエンティティ3,4は、分離された項目として層N+1から下位へ送られた各サービスデータユニットSDUを操作する。これに対し、対等プロトコルNが接続指向型の場合には、関連するプロトコルエンティティ3,4は、層N+1から下位へ送られたサービスデータユニットSDUに関する高信頼性のストリーム伝送サービスを提供する。一般に、ほとんどの対等プロトコルは無接続型であり、１つ又は２つの主要な対等プロトコルだけが接続指向型となる。

上位の層N+1中の多数の異なるプロトコルエンティティにサービスを提供するために、層N中のプロトコルエンティティが必要となることがある。このため、一般に、第１エンドシステムの層N+1中のエンティティが、第２エンドシステム中の対等エンティティにプロトコルデータユニットPDUを送る際に、宛先の対等エンティティの適当な識別を特定層Nのサービスに提供し、即ち、第１エンドシステムのエ

ンティティを提供することにより、第2エンドシステムの層N中の対等エンティティが層N+1中の適当なエンティティにPDUを送ることができるようにする必要がある。

例えば、或るエンドシステムの層N+1中のプロトコルエンティティもまた、多数の他のエンドシステムにおける対等エンティティと通信を行うために必要となることがある。この場合に、層Nのプロトコルが接続指向型である際には、勿論、宛先の層N+1のエンティティの同一性を単に参照することのみにより現在の接続を追跡することは、層Nのプロトコルエンティティにとって適切ではない。そうではなく、接続は、出所エンティティの同一性と宛先エンティティの同一性との組み合わせを参照して頻繁に識別される。

本発明は、層Nのプロトコルエンティティのサービスを利用してプロトコルデータユニットを伝送することによる、例えば層N+1中の、エンティティ間の通信に関するものである。ここで、前記層Nの対等プロトコルは接続指向型のものである。下記の説明では、接続指向型プロトコルの一例として公知の伝送制御プロトコル(TCP)が使用され、このプロトコルは、インターネットプロトコル(IP)と連携して使用される。

TCP/IPネットワークにおいて、TCP層のエンティティは、接続を識別するためにエンドポイントの対を用いる。ここで、1つのエンドポイントは、関連するエンドシステム（即ちより正確にはネットワークに対するエンドシステムのインタフェース）を識別するパラメータ（IPアドレス）と、TCPプロトコルエンティティが通信を行うことになるエンドシステム中の出所／宛先エンドポイントを示すパラメータ（TCPポート番号）とを組み合わせたものである。TCP接続の識別のより詳細な説明は「Internetworking with TCP/IP」（Douglas E. Comer, Volume I, Second Edition 1991, Prentice-Hall）等の参考文献に記載されている。

図2は、TCP/IPプロトコルに従って、或るエンドシステム中のエンドポイントエンティティAから別のエンドシステム中の対等エンドポイントエンティティB（図示せず）へネットワークを介して伝送するためにプロトコルデータユニット(PDU)20が生成される態様を示しており、適当なTCP接続が既に確立されているものと仮定している。図示のとおり、PDU20は、ネットワークを介して受信側エンドシステムに伝送される前に3つのプロトコル層（TCP層22、IP層23、及びネットワークインタフェース層24）を介して下位へ伝送される。各層中では、後に詳述するように、カプセル化プロセスが行われる。単純化のため図2には図示していないが、断片化プロセスもまた1つ以上の層で行われ、その場合、層により受信されたデータは、次の層に送られる前に幾つかのユニットに分割される。

図2に示すように、TCP層プロトコルの基本プロトコルデータユニットは、TCPヘッダ26及びTCPデータ領域27から成るTCPセグメント25である。エンドポイントエンティティAからTCP層22へと下位へ送られるPDU20は、TCP層22のためのサービスデータユニットを構成し、またTCPセグメント25のTCPデータ領域27を形成する。TCPヘッダ26は、多数の情報フィールドを含んでおり、そのうち、本発明に関連するフィールドだけが図示されている。これらのフィールドは、エンドポイントエンティティAのTCPポート番号を保持する出所ポートフィールド28と、PDU20が送られている宛先エンドポイントエンティティBのTCPポート番号を保持する宛先ポートフィールド29と、同じ接続についての別のTCPセグメントに対する現在のTCPセグメント25に関するシーケンス番号を含むシーケンス番号フィールド30と、現在の接続に関連して対等TCP層22から次に予想されるセグメントのシーケンス番号を含む応答番号フィールド31と、種々の制御コードを含むコードフィールド32である。

各TCPセグメント35は、その層のサービスデータとして、IP層23へと下位に伝送される。IP層23の基本プロトコルデータユニットは、IPヘッダ36及びIPデータ領域37から成るIPデータグラム35である。IPデータ領域37は、TCP層22から受信されたサービスデータユニット、即ちTCPセグメント25により占有される。本発明に関連するIPヘッダのフィールドは、送信側のエンドシステムのIPアドレスを示す出所IPアドレスフィールド38、及び、受信側のエンドシステムのIPアドレスを含む宛先IPアドレスフィールド39である。TCP層22に対して出所及び宛先IPアドレスが利用可能とされ、これにより、TCP層22が、出所及び宛先のエンドポイントエンティティに関する一対のIPアドレス及びTCPポート番号に基づいて接続を識別できるようになる。

実際には、TCPセグメントの断片化を行わずにTCPセグメントとIPデータグラムとの間に一対一の対応関係があることが多い。簡略化のため、以下ではそのような構成を仮定する。

ネットワークインタフェース層24は、下層にある物理的な送信ネットワークの特性をそれより高レベルの層に適合させる役割を果たす。このネットワークインタフェース層24は、IPデータグラム35をサービスデータユニットとして受信するように構成されている。ネットワークインタフェース層24の基本プロトコルデータユニットは、フレームヘッダ46及びフレームデータ領域47から成るフレーム45である。フレームデータ領域は、IP層23から受信されたサービスデータユニット、即ちIPデータグラム35によって占有される。

図2に示す場合、物理的ネットワークに現れる各フレーム45は、互いに通信を行うためにTCP層22のサービスを利用して、出所及び宛先エンドポイントエンティティのIPアドレス及びTCPポート番号を含むことが理解されよう。ここで、それらパラメータは、関係するTCP接続を一般的に識別するのに充分なものである。実際には、幾つかのフレームに跨がって各IPデータグラムを断片化することができる。しかし、一般には、IPデータグラムの第1断片を保持するフレームは、その断片がデータグラムのヘッダだけでなくデータグラム中にカプセル化されたTCPセグメントのTCPヘッダも含むのに充分なサイズを有するものである。下記の説明ではこのことを前提とする。

前述したように、TCP層22は、上部の層、即ち図2のエンドポイントエンティティAに接続指向型の通信サービスを提供する。従って、エンドポイントエンティティA,B間の通信の全般的な通抄は次のように行われる。エンドポイントエンティティAがTCP層22のサービスを要求すると、TCP層22は、エンドポイントエンティティBを含むエン

ドシステム中の対等TCP層との接続を確立する。この接続が確立されると、PDU20は、エンドポイントエンティティA及びその対等エンティティBの両者が通信を終了するまで、それらのエンティティ間で伝送される。その後、TCP層はその接続をクローズする。図３は、TCP接続の確立及びクローズに伴うハンドシェークを示すものである。同図では、エンドシステム1,2におけるTCP対等エンティティについて考察している。

図３の上半部は、TCP接続のオープンに伴うハンドシェークを示している。本実施例では、エンドシステム1中のTCP層エンティティは、TCPヘッダ26のコードビットフィールド32にSYNビットがセットされたセグメント25をエンドシステム2中の対等エンティティに送ることにより、接続のオープンを開始する（矢印50）。このセグメントを受信すると、エンドシステム2中のTCPエンティティは、SYN及びACKビットがセットされたセグメントで応答する（矢印51）。この応答が、エンドシステム1中のTCPエンティティにより良好に受信された結果として、完了したハンドシェークセグメントがエンドシステム1からエンドシステム2に送られ、そのエンドシステム2においてコードビットフィールド32中のACKビットがセットされる（矢印52）。これは、接続が確立されたことを双方の側が認識した旨をエンドシステム2に通知する役割を果たす。このハンドシェークの間に、シーケンス番号の送信及び応答が行われて、再接続中に交換されるセグメントの後続の追跡が可能となる。それらのシーケンス番号及び応答番号は、TCPヘッダ26のフィールド30,31に収容される。

図３の下半部は、TCP接続のクローズに伴うハンドシェークを示すものである。接続のクローズは２ステージで行われ、最初に、或る一方向に関する送信側のTCPエンティティが伝送すべき更なるデータを有さない場合にその方向において接続がクローズされ、次いで、他方のTCPエンティティがデータ送信を終了した際に他方向においてクローズされる。図３の例では、エンドシステム1中のTCP層エンティティは、最初に、接続のクローズを所望し、そのためにTCPヘッダ26のコードビットフィールド32中にFINビットがセットされたセグメント25を送る（矢印53）。このセグメントを受信したことは、やがて、ACKビットがセットされたセグメントを返すことにより、エンドシステム2中のTCPエンティティにより応答される（矢印54）。次いで、エンドシステム2中のTCPエンティティは、通信を行うべきデータがなくなるまで、データを保持するセグメントを送り続ける。通信を行うべきデータがなくなった際、エンドシステム2中のTCPエンティティは、FIN及びACKビットがコードビットフィールドにセットされたセグメントを送る（矢印55）。このセグメントがエンドシステム1中のTCPエンティティにより良好に受信されたことは、ACKビットがセットされた最終セグメント25を送ることにより応答される（矢印56）。

エンドシステム1,2のTCPエンティティ間で任意の接続が確立される過程で、図３に示すオープン及びクローズに関するハンドシェークによって定められるような所定パターンのコードビットが、連続するセグメントのコードビットフィールド32中に生じることが理解されよう。

図４は、本発明を実施した呼出記録生成器61を示すものであり、この呼出記録生成器61は、ネットワークに亘って一時的に確立される各TCP接続（又は呼出）の記録を提供するために、ネットワーク60を監視するよう接続されている。図示の通り、呼出記録生成器61は、ネットワーク60に接続されたネットワークインタフェースユニット62と、プロセッサ65及びメモリ64を含む処理サブシステム63とから構成されている。メモリ64は一般に、作業用RAMメモリと、プログラム格納用のROMメモリと、ディスクメモリとから成る（簡略化のため、これらの要素は図４には個別に示さない）。

ネットワークインタフェースユニット62は、ネットワーク上に現れる各フレーム45を捕捉し、処理のためにそれを処理サブシステム63に送る。

図４に示すように、処理サブシステム63は、４つのメインデータ構造66～69を利用して、４つのメイン処理70～73を実行する。

より詳細には、フレームが処理サブシステム63に送られると、処理ステップ70が（例えば割込サービスルーチンとして）開始されて、フレームからデータグラム情報が抽出され、そのデータグラムが、タイムスタンプと共に、データ構造66により構成されたバッファ内に格納される。格納されたデータグラム情報は、一般に、対象となる情報、即ちIPヘッダ及びカプセル化されたTCPセグメントのヘッダのみから成る。更に、データグラムが断片化されている場合には、IPヘッダ及びカプセル化されたTCPセグメントのヘッダを含む第１断片のみが処理され、その他の断片は全て廃棄される。

バックグラウンドで実行されるプロセス71は、新たな項目に関してバッファ66を継続的に監視し、１つ以上の項目が示される毎に、処理用の先頭項目を抽出する。以下で詳述するように、このプロセスには、先頭項目のデータグラムが関する接続を識別し、次いで、その接続についての対応する呼出記録を更新する、というステップが含まれており、活動状態の接続についての呼出記録は、データ構造67により構成された制御ブロックテーブルに保持される。或る接続であって、その接続に関する呼出記録が制御ブロックテーブル67中に存在しないものに、或るデータグラムが対応する場合には、プロセス71により新たな記録が生成される。そのプロセス71は更に、活動呼出記録の別個の関連リストも保持する。このリストはデータ構造68を構成するものである。各呼出記録は、図５を参照して後に詳述するように、対応するTCP接続に関する統計量を含んでいる。

所定間隔で完了走査プロセス72が実行され、これにより、制御ブロックテーブル67中の呼出記録が走査され、所定の最短期間に亘り非活動状態にあった記録が除去される（ここで、「非活動」状態とは、対象となる接続に関連する別のデータグラムの更なる受信に応じて記録が更新されなかったことを意味している）。プロセス72は、呼出記録の関連リスト68を利用して呼出記録の走査を実行する。プロセス72により非活動状態であるものと識別された呼出記録の全ては、データ構造69により構成される完了済呼出記録アーカイブへと除去される（このアーカイブはRAMには格納されず、例えば、ディス

ク記憶装置に保存され、またはオフラインで保持される）。

最後に、オフラインプロセスである呼出記録断片組立プロセス73を使用して、以下で更に詳述するように、実際には同じ接続に関連する呼出記録断片を構成する記録について、アーカイブ69中に含まれる呼出記録を検査する。

呼出記録生成ステップ全体の基本的要件は、勿論、捕捉された各IPデータグラムから一義的な接続識別子を形成できることであり、この識別子は、前記の捕捉されたデータグラムを2つのエンドポイントエンティティの何れが生成したかに関わらず同一となる。本実施例では、プロセス71で生成されたこの一義的な接続識別子は、各々のエンドポイントエンティティの（IPアドレス、TCポート）からなる組によって形成され、この際、数値的に大きいアドレスにポート番号を付加したものが常に最初に配置される。例えば、出所IPアドレスが15.8.61.123、及び出所TCポートが123であり、また宛先IPアドレスが16.8.9.123、及び宛先TCポートが111であるIPデータグラムが捕捉された場合、その結果として生じる接続識別子は、((16.8.9.123.111),(15.8.61.123,123))となる。より一般的には、エンドポイントエンティティAが、バイトaIP1～aIP4から成る4バイトのIPアドレスと、バイトaPort1,aPort2から成る2バイトのTCPポート番号とを有し、また、エンドポイントエンティティBが、バイトbIP1～bIP4から成る4バイトのIPアドレスと、バイトbPort1,bPort2から成る2バイトのTCPポート番号とを有している場合、接続識別子は次のようになる。

((aIP1.aIP2.aIP3.aIP4).(aPort1.aPort2))
((bIP1.bIP2.bIP3.bIP4).(bPort1.bPort2))

ここで、（aIP.aPort > bIP.bPort）である。

この接続識別子は、前述のように、プロセス71により生成される。実際には、接続識別子を直接利用して制御ブロックテーブル67中の対応する呼出記録にアクセスするということはない。これは、その代わりに、接続識別子からハッシュキーが生成されて制御ブロックテーブル67中にハッシングを行うために利用されるからである。本実施例では、使用されるハッシュキーは次の通りである。

（aIP4.bPort2.aPort2.bIP4）

各々の呼出記録の内容を図5に示す。図示の通り、各呼出記録は、その呼出記録が関連する接続についての接続識別子を含む第1フィールドグループと、IPデータグラムが呼出記録の生成を生じさせるプロセス70に関連するタイムスタンプに対応する開始時間フィールドと、呼出記録75の更新に使用された最近に受信されたデータグラムに関連するタイムスタンプに対応する終了時間フィールドと、どのエンドポイントエンティティが接続を開始したかの情報を含む呼出基点フィールドと、記録がなお活動状態にあるか否かを判定するために利用される活動フラグフィールドとを含んでいる。これらの一般フィールドに加えて、各呼出記録75は、二方向の各々における呼出の統計量に関する2つのフィールドグループ77,78を含んでいる。このため、エンドポイントエンティティAに関し、呼出記録75は、Aの物理アドレス（この情報は、呼出記録生成器により受信されてプロセス70によりデータグラム情報と共に格納された各フレームから抽出される）と、そのエンドポイントエンティティAのIPアドレス及びTCPポート番号と、そのエンドポイントAに送られるIPバイトの総数と、Aに送られる全てのTCPフラグの累積集合と、Aに送られる最初のシーケンス番号と、Aに送られる最後のシーケンス番号とを含むフィールドを備えている。エンドポイントエンティティBについての記録75にも、対応するフィールドが存在する。

シーケンス番号が収集される理由は、特定方向に送られたTCバイトの総数を検査するためである。あらゆる所与の方向について、第2シーケンス番号から第1シーケンス番号を減算した値は、その方向に送られたTCPバイトの総数の概算指示を表わすものとなる。この指示が概算値に過ぎないのは、TCPデータは存在しないがシーケンス番号が1だけインクリメントされる場合、即ちACKセグメントが存在するからである。プロセス73により行われる呼出記録断片の再組立を容易化するために、認められた全てのTCPフラグの集合が収集される。

次に、プロセス71による呼出記録の生成及び更新について、図6に示すフローチャートを参照して一層詳細に説明する。プロセス71は、開始されると、データグラムがその関連するタイムスタンプと共にバッファに入力されていることを検出するまで、継続的にバッファ66をチェックする（ステップ81）。その後、プロセス71は、バッファ66から先頭項目を取り出して（ステップ82）、その先頭項目データグラムについて接続識別子を構成する（ステップ83）。プロセス71は更に、その接続について対応するハッシュキーを構成し（ステップ84）、次いでそのハッシュキーを用いて制御ブロックテーブル67へのアクセスを試行する（ステップ85）。開放型ハッシング技術が用いられ、即ち、ハッシュテーブル67中の各項目毎に別個のオーバーフロー領域を維持することによって衝突分解能(resolution)が達成される。ハッシュキーによって示されるロケーションに項目が見つからない場合には、処理中のデータグラムは新たな接続に関するものであると仮定される（ステップ86）。しかし、ハッシュキーによって示されるロケーションに、一致する項目が見つかった場合には、そのデータグラムは、そのロケーションにおける呼出記録に関連する接続に関するものであると仮定される。

最初に、新たな接続が仮定される状況を考察した場合、プロセス71は、制御ブロックテーブル67中に新たな呼出記録75を生成し（ステップ87）、活動記録リスト68を更新する（ステップ88）よう進行する。新たな呼出記録を生成する際に、プロセス71は、対応する記録フィールドに接続識別子を入力し、また開始時間フィールド及び呼出基点フィールドを満たす（ステップ89）。既述のように、開始時間フィールドは、呼出記録の生成を開始させるデータグラムに関連するタイムスタンプを保持するために使用される。呼出記録75の呼出基点フィールドは、接続のどのエンドポイントエンティティが呼出の基点になったかの指示を含んでいる。この情報は、呼出記録の生成を開始させるデータグラム中のTCPコードビットから推論される。この最初のデータグラムは関連するTCP接続の確立に一般に伴う

ものとなると解されるので、TCPヘッダ中のコードビットは、図3の上半部に示すシーケンスを辿ることになる。特に、考慮すべき3つの主な場合がある。

1．TCPコードビットがSYNしか含まない場合。このことは、それが接続についての最初のデータグラムであり、従って、接続基点はそのデータグラム中の出所アドレスによって識別されるエンドポイントエンティティである、ということを意味している。

2．TCPコードビットがSYN及びACKの双方を含んでいる場合。これは、データグラムが接続要求への応動に関連するものであり、従って、接続についての基点エンティティはそのデータグラムの宛先アドレスによって識別されるものである、ということを示している。

3．コードビットがSYNを含んでいない場合。これは、接続確立ステップに失敗したことを示している。

上記3つの場合のうちの最後の場合では、呼出記録75の呼出基点フィールドは、基点が未知であることの指示を含むよう設定される。

新たな呼出記録75を生成する際、プロセス71はまた、各エンドポイントエンティティ毎に、そのエンティティの物理アドレスとIPアドレスとTCPポート番号とを入力する。

呼出記録75中の他の項目は、プロセス71によってステップ91,92で生成され、これら項目は、新たに生成される呼出記録と、既存の接続に対応する呼出記録との双方について生成される。ステップ91で、呼出記録の終了時間フィールドが、プロセス71によって処理されているデータグラムのタイムスタンプにセットされ（勿論、新たに生成された呼出記録の場合、その終了時間はその開始時間に対応する）、更に、呼出記録の活動フラグがセットされる。ステップ92では、受信側のエンドポイントエンティティに関する統計量が更新される。特に、まだ存在しない場合には最初のシーケンス番号が呼出記録に入力され、TCPバイト数とTCPセグメントとIPバイトとが更新され、累積されたTCPフラグの集合が更新され、認められた最後のシーケンス番号が入力される。

ステップ92が終了すると、プロセス71は、バッファ66で処理されるべき項目のチェックに戻る（ステップ81）。

このようにして、プロセス71は、ネットワークに亘って実行される各々の呼出の記録を構築する。

制御ブロックテーブル67中の活動呼出記録のグループから維持されている接続に対応する呼出の除去は、完了走査プロセス72により行われる。このプロセス72を図7にフローチャートで示す。より詳細に述べると、割込タイマによって設定される周期的な時間間隔（例えば3分に一度等）でプロセス72が開始され（ステップ100）、次項目ポインタが、活動呼出記録リスト68の先頭を指すように初期化される（ステップ101）。その後、次項目ポインタにより指されたリスト項目がフェッチされ（ステップ102）、その次のリスト項目（存在する場合）を指すように次項目ポインタが更新される。次いで、前記のフェッチされたリスト項目により識別される呼出記録の活動フラグが検査される（ステップ103）。この活動フラグがリセット状態にある場合、これは、完了走査プロセス72の最後に実行されてから呼出記録が生成または更新が行われていないことを示している（活動フラグは呼出記録の生成／更新中にプロセス71によりセットされるものであることが理起される）。これらの記録は、完了した接続に関するものであると解され、従って、プロセス72は、テーブル67に保持されている活動呼出記録グループから前記記録を除去し、それら記録を完了済呼出記録アーカイブ69に転送する（ステップ104）よう進行する。その後、プロセス72は、その転送された呼出記録に対応する項目を除去することにより、活動呼出記録リスト68を更新する。

また、ステップ103でチェックされた呼出記録の活動フラグがセット状態にある場合には、対応する接続が依然として活動状態にあり、呼出記録が制御ブロックテーブル67に残っているものと仮定される。しかし、その活動フラグはリセットされる（ステップ106）。

ステップ105又はステップ106が適正に終了した後、プロセス72はステップ108に進み、同ステップで、次項目ポインタにより示される更に別の項目がリスト68中に存在するか否かのチェックが行われる。更に別の項目が存在する場合、プロセスはステップ102に戻る。しかし、リスト中の全項目の処理が終了している場合には、プロセス72は、プロセス72による連続的走査の間の期間を計時するために割込タイマを再始動させて（ステップ109）、次いで終了する（ステップ110）。

既存の呼出記録が、連続的走査の間の期間中に更新されない場合には、その呼出記録は、後の完了走査プロセス72の実行中に、制御ブロックテーブル67中に保持された活動呼出グループから除去される、ということが理解されよう。本実施例では、プロセス72の連続的な実行の間の間隔は3分である。しかし、3分以外の間隔とすることも可能である。但し、TCP保属(keep-alive)パケットが或る種のTCP接続に送られる期間が45秒であるため、前記間隔は45秒より長くすべきである。間隔の選択は、つまるところ、アイドル／完了接続に関するテーブル67中の使用済スペースと、活動呼出記録を走査するのに必要な時間の量と、以前に生成された不完全な呼出記録から完全な呼出記録を構築するために実行する必要があるオフライン呼出記録断片再組立（図4のプロセス73）の量との間でトレードオフを決定することになる。上述のプロセス72の利点は、特定のTCP接続に関して送られるべき最後のデータグラムであるか否かを判定するために全てのデータグラムをチェックする必要を除くし、これにより、1データグラム当たりの処理時間が削減されることにある。更に、プロセス72は、接続クローズシーケンスを含むデータグラムが損失された場合であっても依然として有効なものである。

勿論、接続が、完了走査プロセス72の連続的な実行の間の間隔より長い間アイドル状態であるべき場合には、対応する呼出記録は、接続が完了する前にテーブル67から除去されることになる。次いで、接続トランザクションの残りの部分は、別個の接続としてログが形成されてそれ自体の呼出記録が生成される。その結果として、同じエンドポイントのエンティティ間の多数の部分的に完成した呼出記録が生成可能となる。しかし、呼出記録断片アセンブリプロセス73

が用いられて、各呼出記録のTCPフラグフィールドに記録されたコードビットを参照することにより前記の呼出記録断片の再組立が行われる。より詳細に述べると、TCPフラグリストと開始及び終了時間とを使用することにより、プロセス78は、呼出記録断片をつなぎ合わせて一組の完全な呼出記録を作成する。例えば、呼出記録は3つの呼出に分割可能であり、各々の呼出記録のTCPフラグリストは次の通りとなり得る。

記録1 －SYN,ACK,PUSH

記録2 －ACK,PUSH

記録3 －ACK,PUSH,FIN

SYN,ACK,FINを（図3を参照）、また一般にはPUSHをも含むフラグリストを通常の呼出が有するべきである場合、上記の3つの呼出記録が同じ接続についてのものであるということはかなり確実である（但し、開始及び終了時間は適切に一致するものとする）。勿論、このプロセスは、あらゆる呼出断片が良好にピックアップされることを保証するものではないが、大多数は良好にピックアップされることになる。

上述の呼出記録生成及び監視方法には多くの変更が可能であることが理解されよう。特に、本呼出記録生成及び監視方法は、TCP接続以外の接続の監視にも適用可能であることが理解されよう。更に、呼出記録生成器にフィルタを組み込んで或る範疇のフレームをフィルタリングすることにより、例えば、呼出記録生成器が、特定のネットワークのノードまたはサブネットワークから発せられた呼出に関する記録だけを生成するようにすることができる。呼出記録生成器の詳細な実施態様に関し、考えられる一つの変形例としては、完了定査プロセス72について各呼出記録の終了時間フィールドを利用して対応する接続が依然として活動状態であるか否かを判定する、という方法がある。この場合、終了時間フィールドの内容はタイムスタンプのタイミング源により得られる現在時間と比較されることになる。このような構成により、活動フラグフィールドが不要となる。別の可能な変形例としては、活動呼出記録と完了呼出記録との双方を同じメモリに格納して、各記録に関連する適当なフラグにより各グループの要素を互いに区別する、という方法がある。更に、活動呼出記録にアクセスするために必ずしもハッシュテーブルを使用する必要はない、ということが理解されよう。

FIG 1

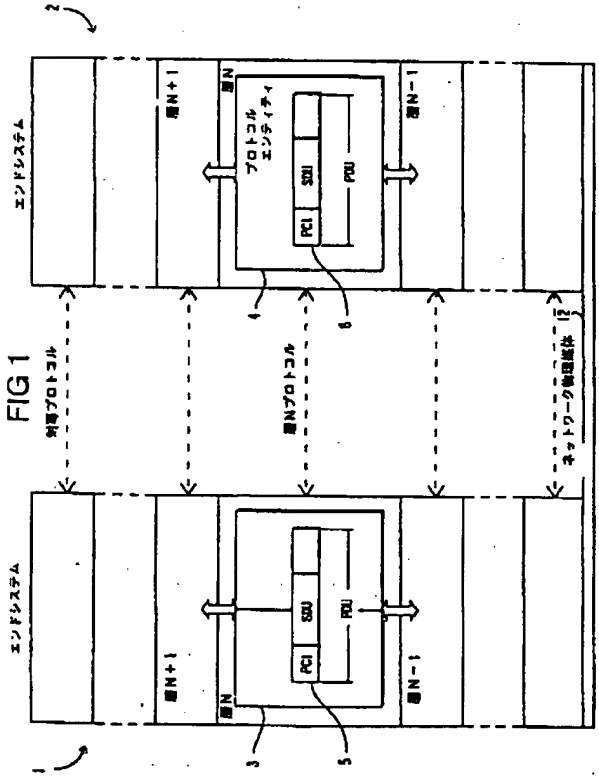
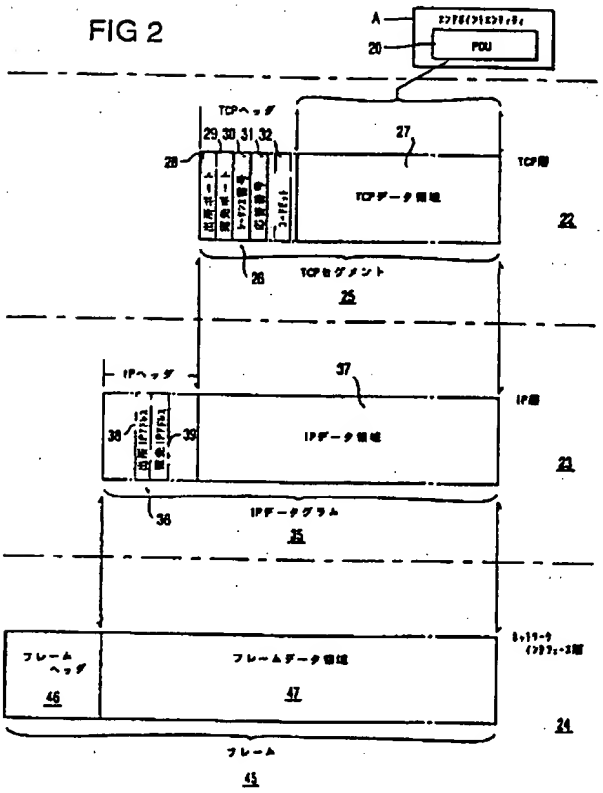


FIG 2



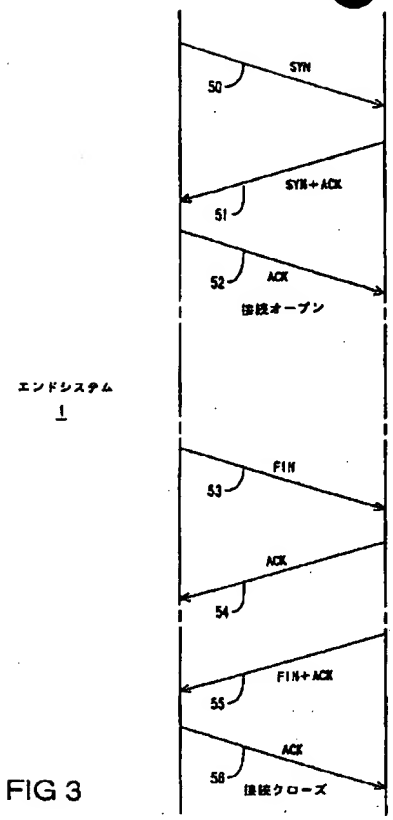


FIG 3

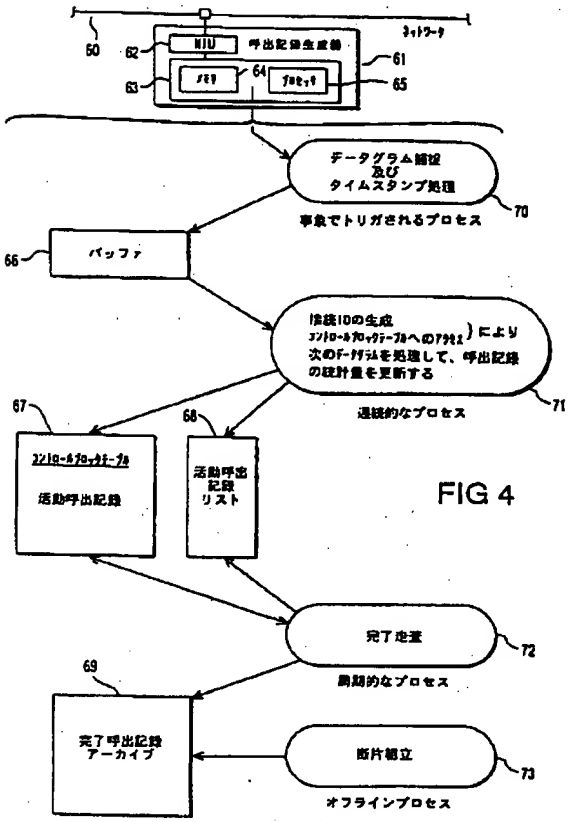


FIG 4

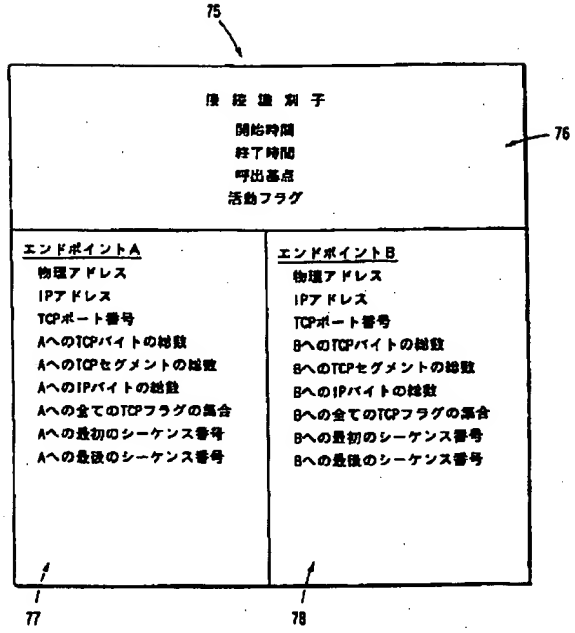
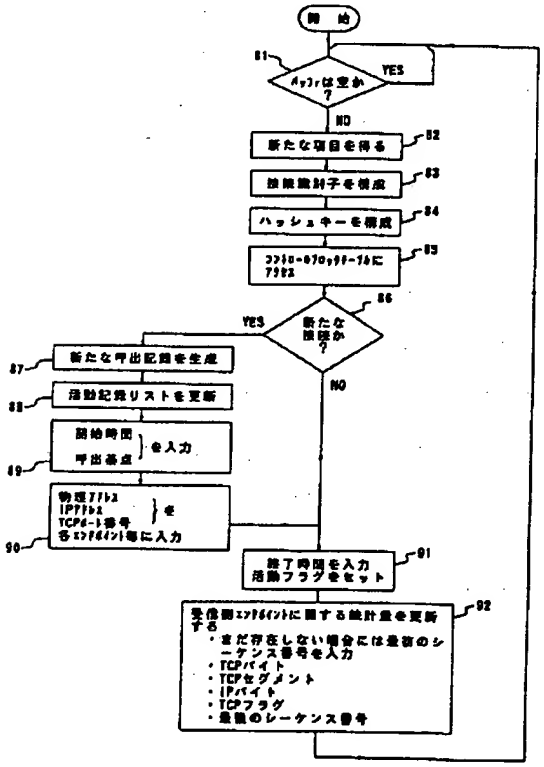
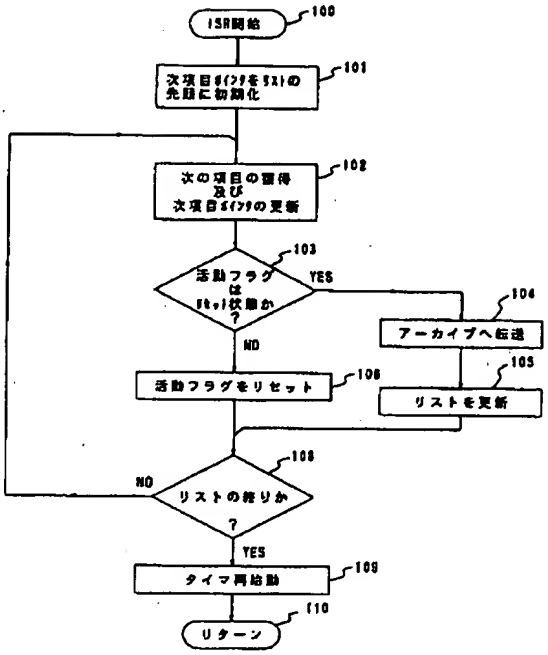


FIG 5

FIG 6



F I G 7



国 際 調 査 報 告

PCT/GB 92/01090

I. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. 5 H04L29/06

II. FIELDS SEARCHED

Classification System	Classification Symbols
Int.Cl. 5	H04L

III. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	10TH CONFERENCE ON LOCAL COMPUTER NETWORKS 7 October 1985, IEEE, NEW YORK, US pages 32 - 40 C.COTTON 'Methods for internet monitoring' see page 33, right column, line 30 - line 32 see page 35, line 17 - line 28	1,12
A	EP,A,0 467 569 (D.E.C.) 22 January 1992 see column 3, line 16 - line 43 see column 4, line 1 - line 51	1,2,12
A	EP,A,0 478 175 (HEWLETT-PACKARD) 1 April 1992 see column 3, line 8 - line 55 see column 5, line 13 - line 56	1,12

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
18 JANUARY 1993	04.02.93
International Searching Authority	Signature of Authorized Officer
EUROPEAN PATENT OFFICE	DE LA FUENTE DELAQUA

国 際 調 査 報 告

GB 9201090
SA 60970

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 18/01/93

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0467569	22-01-92	JP-A- 4233845	21-08-92
EP-A-0478175	01-04-92	EP-A- 0474932	18-03-92

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI
H04L 29/14			